cymulate

DATA SHEET

Automated Exposure Mitigation

Go Beyond Validation to Mitigate Threat Exposure

Security teams know they are in a daily race to stay ahead of advanced cyber threats. To harden defenses before the next attack, Cymulate delivers the insight and automation needed to continuously optimize prevention. With automated control updates based on validated threat exposure, organizations can maintain resilience against evolving threats.

The Cymulate Exposure Management Platform is the trusted solution for continuously testing and validating security controls and policies. It leverages automated threat emulation powered by the latest threat intelligence, real-world vulnerability exploits and full coverage of MITRE ATT&CK tactics and techniques.

For identified security gaps, the Cymulate platform includes the option for automated exposure mitigation that pushes updates to security controls to block or detect the missed threat. Through the combination of threat validation and automated control updates, Cymulate automates the process of:

- Daily testing of new threats
- Updating security controls to block validated threats
- Proving threat resilience and the current state of security posture

From Exposure to Mitigation with Immediate Prevention

With a daily update of the latest threats, Cymulate closes the loop between validation and prevention by including the automated mitigation option for immediate control updates.

As Cymulate validates exposures and identifies security gaps, automated mitigation deploys targeted updates, pushing relevant indicators of compromise (IOCs), such as file hashes, registry keys and URLs directly to connected security controls. This process transforms validation into threat prevention while reducing your time to mitigate.

> **Cymulate integrates with our XDR to improve our threat detection and response. Cymulate automatically uploads critical threat data directly to our XDR to ensure that potential threats are identified and addressed quickly, without manual intervention.**
>
> – Senior Security Manager, Singapore Bank

Benefits

Mitigate Faster

Reduce manual tasks with automation that converts exposure validation to immediate threat resilience.

Optimize Prevention

Push threat updates directly to security controls to block threats that have been proven to bypass your security controls.

Operationalize CTEM

Drive continuous threat exposure management with automation to mitigate validated threat exposure.

Reduce Dwell Time

Develop self-improving defenses that evolve in response to changing threat landscapes.

How It Works

Cymulate streamlines the mitigation process with flexible options that cater to workflow and level of automation readiness. Whether teams prefer direct control or full automation, the platform's mitigation methods ensure faster, safer and more efficient response to validated exposures. Once IOCs are pushed to the relevant controls, Cymulate can automatically retest those defenses to confirm that the mitigation is effective, providing immediate validation and proof of improved resilience.

Fix with a click

For targeted action, users can review individual findings and select specific mitigations to push directly to security controls. This option provides hands-on precision, enabling security teams to address critical exposures immediately while maintaining full oversight.

Bulk fix with a click

Aggregate mitigations from an assessment or multiple assessments to group recommended IOCs into a single bulk update. This approach is ideal for quickly updating defenses after broad validation tests or widespread threat simulations.

Auto-fix

For organizations seeking full automation, auto-fix allows predefined rules and parameters, such as time-based triggers, control types or mitigation categories, to govern automatic updates. This ensures continuous alignment between validation results and active defenses, keeping controls up to date with minimal manual effort and verifying each update through automated retesting.

Integrate with Security Controls to Harden Defenses

The Cymulate option for auto mitigation includes control integrations for:

Vendor	Solution	Vendor	Solution
CROWDSTRIKE	Crowdstrike Falcon	TREND MICRO	Trend Micro Vision One
Microsoft	Microsoft Defender for Endpoint	SentinelOne	SentinelOne Singularity Endpoint
paloalto NETWORKS	Palo Alto Cortex XDR		

Why Choose Cymulate?

Depth of attack scenarios

Over 100,000 attack simulation resources from real-world attack scenarios for comprehensive testing of your security defenses.

Production-safe execution

The full suite of attack simulations and test scenarios are completely production-safe and will not cause harm to your production systems.

Adapt to new threats

Actionable and automated findings to maximize threat prevention and optimize detection for the most effective threat coverage.

Contact us for a live demo Start Your Live Demo info@cymulate.com www.cymulate.com